THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

Law in the Last Mile

Citation for published version:
Mac Sithigh, D 2009, 'Law in the Last Mile: Sharing Internet Access Through WiFi', *SCRIPTed*, vol. 6, no. 2, pp. 355-376. https://doi.org/10.2966/scrip.060209.355

Digital Object Identifier (DOI):
10.2966/scrip.060209.355

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
SCRIPTed

Publisher Rights Statement:
© Mac Sithigh, D. (2009). Law in the Last Mile: Sharing Internet Access Through WiFi. SCRIPTed, 6(2), 355-376. 10.2966/scrip.060209.355

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 07. May. 2023

scripted

Volume 6, Issue 2, August 2009

Law in the Last Mile: Sharing Internet Access Through WiFi

Daithí Mac Síthigh[*]

Abstract

Access to the Internet through wireless access points (typically wifi routers) is both simple and common. In this paper, the legal restrictions on "sharing" an Internet connection in this way are assessed. Criminal offences that could apply to the use of open networks, such as dishonest use of a communications service or unauthorised access to a computer, are considered, as are issues of criminal and civil liability and terms of use affecting the owner of the router. It is suggested that there are advantages to sharing and that these provisions unnecessarily restrict the development of what would be of benefit to society. Furthermore, the problems encountered by proponents of municipal and community networks based on a collection of wireless access points, in terms of competition law but also other matters, are summarised. The paper concludes with an assessment of the links between the various aspects of wireless Internet policy, suggesting that it is necessary to recast relevant legal provisions so as to avoid granting disproportionate protection to Internet service providers (ISPs).

[This article was presented at the SCRIPTed "Governance of New Technologies" conference held in Edinburgh on 29-31 March 2009.]

DOI: 10.2966/scrip.060209.355

© Daithí Mac Síthigh 2009. This work is licensed under a Creative Commons Licence. Please click on the link to read the terms and conditions.

---

[*] Lecturer, University of East Anglia. This paper was presented at the SCRIPTed conference, "Governance of New Technologies," Edinburgh, 29-31 March 2009. The author thanks Burkhard Schafer (University of Edinburgh) for chairing the panel, those who offered questions and suggestions, and Oisín Tobin (Merton College, Oxford) for very useful comments on an earlier draft.

1. Introduction

In this paper, it is argued that the adoption and full realisation of the benefits of new technologies supporting wireless use of the Internet are constrained by a diverse range of legal provisions. The focus is on the problems relating to sharing Internet connectivity through wireless access points. Consideration is also given to the difficulties encountered by proponents of municipal and community wifi networks. The scientific advantages of enhanced wireless connectivity are shown to be in conflict with some of these established legal norms although, in the context of information technology (IT) law more generally, other philosophical and practical challenges do of course exist. The developing issue of so-called "white space" Internet access is briefly explored, considering whether this debate shows a maturing in the approach of legal systems to the use of wireless technologies in the "last mile" between backbone/ISP networks and the individual user.

It is contended that while technological novelty cannot be considered in isolation, and wireless technologies do not solve every problem, the key problem is that "Internet access" is not, as yet, treated in a way that enables the full exploitation of the potential of wireless solutions. This is particularly true in the cases of the legal provisions discussed in this article, e.g. the individual issues encountered by the casual user and the difficulties presented by competition law considerations to municipal planners. In a world where wireless Internet access itself has been the subject of rapid development, with the ability to watch video[1] being a particularly important example, this suggests that there are many opportunities for Internet access to become a substitute for (or complement to) traditional broadcast consumption – if this is not already the case.

This is especially the case where the metaphors in use are inappropriate and lead legal authorities, in particular, to bring unnecessary criminal charges or restricting actions in the public interest. The question of metaphors is a familiar one, and has been discussed in particular in the case of copyright.[2] It is already proving a relevant one, too, in terms of the policy issues associated with wireless access.[3] Ultimately, the choices made have an impact on the construction of contemporary public, cultural and virtual spaces and therefore are a matter of social importance beyond the undoubtedly interesting questions of IT law that arise.

In section 2, I set out the benefits of sharing, alongside the various associated objections and concerns. Drawing upon these "mixed messages," I consider the legality of using (section 3) and providing (section 4) an open wireless access point.

---

[1] K Greene, "High-Definition Video over Wi-Fi" (*Technology Review* Feb 2009) available at http://www.technologyreview.com/computing/22195/ (accessed 6 April 2009)

[2] B Herman, "Breaking and entering my own computer: the contest of copyright metaphors" (2008) 13 *Communication Law & Policy*, 231-274.

[3] A Powell, "The public utility and the public park: Metaphors and models for community-based Wi-Fi networking" [2008] *IEEE: Technology & Society* available at http://ssrn.com/1330913 (accessed 6 April 2009); R Cannon, "Steal More Wifi!" (2009) available at http://ssrn.com/1333404 (accessed 6 April 2009), at 22-23.

Finally, section 5 includes a discussion of other approaches to wireless connectivity, focusing on the use of multiple access points in "municipal wi-fi" networks.

2. Why share?

Wireless access points (often referred to as "wifi routers" or similar; the abbreviation WAP is used in this article) are available in retail outlets, often supplied by ISPs to new customers and inexpensive. The vast majority of laptops currently sold to customers (whether domestic or business) have wifi functionality built in as standard and a wide range of other devices (such as iPhones) are similarly equipped. Communication between WAPs and suitable devices is normally by way of permitted use in an unlicensed spectrum, such as in the 2.4GHz band,[4] and certain standards (such as the IEEE's family of 802.11 protocols) and certifications (most notably, that of the Wi-Fi Alliance) are in use.

While there are many other uses to which a WAP could be put by the person using it (for convenience, referred to here as the "WAP Admin"), the most recognisable one is the "sharing" of a single Internet connection (typically delivered through DSL or cable by a retail ISP). Indeed, in many cases the WAP admin (who is also the customer of the ISP) will simply connect a suitable ISP-supplied modem to the point of cable or DSL entry to the home and the WAP to the modem, and use it exclusively for enabling laptops and other devices to connect to the Internet. The WAP can be open (i.e. any device can connect to it), secured through one of a range of options such as wired-equivalent privacy (WEP) or wifi protected access (WPA), or open but subject to controls on access to the Internet (browser-based authentication). By design, sharing is possible; furthermore, consumers are notified that "going wireless" carries with it significant benefits (e.g. being liberated from a single, fixed connection point).

The first question we must address, then, is what are the problems associated with this simple system.[5] There are many who mix enthusiasm with caution. For example, the Commission for Communications Regulation (Comreg) in Ireland sets out the advantages of "home networks" (of which wireless networks are cited as one example):[6] the reduction of the need for equipment and wires; the possibility for including everything from security systems to kitchen appliances in the network; and the ease with which services like Internet protocol TV (IPTV) can be delivered to the home. It is added that "Internet connection sharing" is an advantage, while "security" is a challenge – "with hacking and phishing becoming more prevalent, it is crucial that the appropriate security measures are put into place to protect the network (the wireless network range may spread outside of your house)."

---

[4] In the United States (US), 47 CFR 15.247; in the European Union (EU), ERC Decision 01/07.

[5] The literature to date focuses on the position in the US, but is still of quite some value. See: B Kern, "Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law" (2005) 21 *Santa Clara Computer & High Tech Law Journal*, 101-162; R Hale, "Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet" (2005) 21 *Santa Clara Computer & High Tech Law Journal*, 453-559; M Bierlein, "Policing the wireless world: access liability in the open wifi era" (2006) 67 *Ohio State Law Journal*, 1123-1185.

[6] Commission for Communications Regulation, "Quarterly Key Data Report: Q3 2008" available at http://www.comreg.ie/_fileupload/publications/ComReg08101.pdf (accessed 6 April 2009).

This statement deserves further investigation. The advantages of wireless technology are being presented as promoting domestic convenience and enabling the home user to take full advantage of the commercial services offered by telecommunications providers. Indeed, the split between internal co-operation (printer sharing, wifi-enabled fridges and the like) and external exclusion (security being crucial) is quite remarkable. A domestic network is thus sanitised and enables the household to buy more services (or make good use of existing services) without challenging the business model of the provider.

It is therefore useful to consider the Comreg statement as a warning of possible "dangers." Certainly, with acknowledged issues relating to the security of an open network, a national regulatory authority (rather than an ISP, which would have obvious, selfish reasons to discourage any sharing) can clearly make an impact on user behaviour. The key issue here is that when an individual makes use of an open WAP, they may be able to use that WAP to access information on other machines using that WAP or connected to the domestic network. Therefore, statements by experts about possible criminality and antisocial activities on the part of the person who takes advantage of the sharing are no doubt treated with some seriousness (and reported dutifully by non-specialist media). The chief technology officer of a well-known computer security company (Sophos) argues that

> *Stealing Wi-Fi internet access may feel like a victimless crime, but it deprives ISPs of revenue. Furthermore, if you've hopped onto your next door neighbors' wireless broadband connection to illegally download movies and music from the net, chances are that you are also slowing down their internet access and impacting on their download limit.*[7]

Whether the advice is based on security, social manners or legal issues, the nature of the threat and the ways in which it can be ameliorated by those who still wish to "share" should form a part of the analysis. In particular, where a public body is involved, protecting its independence from the regulated industry and credibility with the consumer would suggest that it is necessary to approach the "sharing" question with more caution.

For present purposes, the presumption that sharing Internet access (i.e. with the consent or acquiescence of the WAP admin) is wholly without merit is set aside, so that we can proceed with an assessment of where responsibility for such actions lies. This is particularly important in the context of purported illegality associated with sharing. Acknowledging (and explaining below) that open WAPs will be found by walking down a typical city street, or auto-detected and auto-joined by some (legally available) devices, and that attempts to bring these individual facilities together for a collective purpose as mesh networking are popular,[8] certainty in the legal arrangements is desirable. With this in mind, I now turn to consider a question that

---

[7] Sophos, "Wi-Fi piggybacking widespread, Sophos research reveals" (press release, 15 November 2007) available at http://www.sophos.com/pressoffice/news/articles/2007/11/wi-fi.html (accessed 6 April 2009).

[8] K Varnelis (ed), *Networked Publics* (Cambridge, MA: MIT Press, 2008), at 128; see, further, the discussion of FON (note 83 below) and accompanying text.

many users cannot but ask: if they connect to an open WAP and proceed to use it for purposes such as unobjectionable Internet access, do they violate any laws?

3. Is it legal to use an open WAP?

3.1 Obtaining an electronic communications service

The question here is whether use of the Internet through an open access point is a criminal offence. Our starting point is section 125 of the *Communications Act 2003*, which provides that: "A person who- (a) dishonestly obtains an electronic communications service [ECS], and (b) does so with intent to avoid payment of a charge applicable to the provision of that service, is guilty of an offence."

ECS (an aspect of the EU Framework Directive)[9] is elsewhere defined as: "a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except in so far as it is a content service." This is not a general definition of "services," but a specific term of art within telecommunications law. Section 125 is based on section 42 of the *Telecommunications Act 1984*, a statute which put into place certain aspects of the deregulation of telecommunications. Section 42 of the 1984 Act reads: "A person who dishonestly obtains a service to which this subsection applies with intent to avoid payment of any charge applicable to the provision of that service shall be guilty of an offence."

"A service to which this subsection applies" was a licensed telecommunications service, excluding certain broadcast-related services. The statutory intent here is extremely clear – it allows those who use a telecommunications service without paying for it to be held to account for those actions. Cases where this section was material included: the connection of equipment to telephone lines to avoid calls being registered for billing purposes;[10] the placing of calls without payment for the purpose of inflating premium-rate revenues;[11] and, most peculiarly, in *Farrant*, the use of a military-issued mobile telephone by a member of the forces for calls to premium-rate chat lines.[12] But how is this applicable in the case of Internet access?

The conviction of Gregory Straszkiewicz[13] is an example of the successful use of section 125, and a number of published reports indicate that arrests have been made

---

[9] Directive 2002/21/EC of the European Parliament and Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0050:EN:PDF (accessed 6 April 2009).

[10] *R v Levitz*, [1990] 90 Cr App R 33 (CA); another example is the underlying offence in *Morgans v DPP*, [2001] 1 AC 315 (HL), a case regarding the admissibility of intercept evidence, where the defendant placed international telephone calls through a computer system that he had accessed without authorisation.

[11] *R v Boyle*, [1992] 94 Cr App R 158 (CA).

[12] *R v Farrant*, [2003] EWCA Crim 1171. Unfortunately, the matter reached the Court of Appeal in relation to a question of procedure before the Courts Martial; it is surely arguable whether the conduct in question was properly covered by the Telecommunications Act.

[13] Not reported formally as it is a minor, first instance matter. No appeal decisions on this point have been located by the author. Straszkiewicz's conviction, though, was the subject of some media

and cautions issued with reference to the same section.[14] In other cases, however, it is not clear what the alleged offence was.[15] What is particularly interesting about this category of cases is that, as WAP admins are not known or expected to "charge" for the use of their networks, it can only be concluded that the offence is not access to the WAP or the home network, but use of the Internet connection (i.e. access to the wider network), therefore evading the "charge" that the ISP would normally require for connection (a broadband subscription). This would satisfy subsection (b) of section 125 (although the untested finding in *Farrant* might suggest an alternative - if stretched - approach).

This is still an unusual approach and one that would seem to owe more to a theoretical analysis of market conditions (would the user have entered into a contract with the ISP for a subscription were it not for the free alternative?) rather than the enforcement of the criminal law. A user with a subscription to a telephone service would presumably, following this approach, be forbidden from allowing others to use unlimited calling plans as the making of calls by others would be an illegal deprivation of revenue. This is absurd, but is it any more absurd than charging users of open networks? What is important about this is that, if the harm is suffered by the ISP (the party that would receive payment), then the dishonesty is surely also expressed in relation to the ISP. Notwithstanding this, it is hard – impossible, perhaps – to distinguish between the use of an open network without the consent of the ISP's customer (the WAP admin) and use with said consent. It is also unclear what emphasis is placed on the requirement for "dishonest" obtaining of the service: clearly the intention here is to refer to the established body of case law on dishonesty (the *Ghosh* tests – i.e. dishonest by the standards of reasonable, honest people and realising that the behaviour was dishonest by these standards).[16] It is far from certain that either element would necessarily be satisfied in a typical case – particularly in the light of the widespread use of WAPs by reasonable, honest laptop and iPhone users.

The reasonable approach would be to say that the *Communications Act* does not catch this type of behaviour as there is no intent to avoid a (non-existent) charge. However, in the absence of proper consideration by a court, the uncertainty persists. An alternative approach is to charge under the Computer Misuse Act: this has been reported in a number of cases[17] –and is discussed in more detail below – though, in some of the cases reported by the news media, it does appear that the required elements may not have been fully tested. A separate but related point is that users are

---

coverage: e.g. J Wakefield, "Wireless hijacking under scrutiny" (*BBC News* 28 July 2005) available at http://news.bbc.co.uk/1/hi/technology/4721723.stm (accessed 6 April 2009). The individual concerned was accused of using the WAP of a householder by sitting in his car outside their house.

[14] "Two cautioned over wi-fi 'theft'" (*BBC Midlands* 17 April 2007) available at http://news.bbc.co.uk/1/hi/england/hereford/worcs/6565079.stm (accessed 6 April 2009); N Paris, "Two arrested over wifi theft" (*Daily Telegraph* 19 April 2007) available at http://www.telegraph.co.uk/news/uknews/1548960/Two-arrested-over-wifi-theft.html (accessed 6 April 2009).

[15] C Williams, "Broadbandit nabbed in Wi-Fi bust" (*The Register* 22 Aug 2007) available at http://www.theregister.co.uk/2007/08/22/chiswick_wardriver/ (accessed 6 April 2009).

[16] *R v Ghosh*, [1982] QB 1053.

[17] B Ray, "Police collar kid for Wi-Fi pinching" (*The Register* 30 October 2008) available at http://www.theregister.co.uk/2008/10/30/wi_fi_arrest/ (accessed 6 April 2009).

advised to be aware of the dangers of using open networks as the network can be a fake one or subject to monitoring/abuse of some sort.[18]

The origin of section 125 in telecommunications law is part of the problem. Older telecommunications offences have been based on the protection of the integrity of a single national network with clear boundaries and familiar billing systems. This is particularly apparent in the case of Ireland, where the older legislation has been added to and reinterpreted over time rather than replaced by a new offence, as was the case in the UK. The *Postal and Telecommunications Services Act 1983* (creating inter alia a new State-owned telephone company, Telecom Éireann) provides that:

> *A person who wilfully causes the company [Telecom Éireann] to suffer loss in respect of any rental, fee or charge properly payable for the use of the telecommunications system or any part of the system or who by any false statement or misrepresentation or otherwise with intent to defraud avoids or attempts to avoid payment of any such rental, fee or charge shall be guilty of an offence.*[19]

The parliamentary record indicates that this section "penalises the fraudulent or attempted fraudulent use of the telecommunications system. This closes a gap in existing laws."[20] After a series of amendments, the section is still in force, but in a confused fashion. First "the company" was changed to "a licensed operator," reflecting the first stage of liberalisation.[21] Subsequently, by way of statutory instrument transposing the package of EU directives on electronic communications, a reference to a licensed operator has been construed as a reference to an authorised undertaking covered by the minimalist general authorisation procedure.[22] The original definition ("the telecommunications system or any part of the system") is narrow, and is grammatically absurd even after the 1999 amendment (changing to any licensed operator). There is no longer something that, even at that time, we could call "the system." Is there not a distinction between "the telecommunications system" (public) and a broad definition that encompasses a wide range of systems and service providers? Furthermore, there is the explicit reference to "loss" (as distinguished from section 125 in the UK). Section 99(1) in Ireland has indeed been used against a person cloning mobile phone SIM cards, though it was clear in that case that there was loss.[23]

---

[18] D Hobson, "How to use public Wi-Fi safely" (*Out-Law* 16 December 2008) available at http://www.out-law.com//default.aspx?page=9661 (accessed 6 April 2009).

[19] *Postal & Telecommunications Services Act 1983*, s 99(1).

[20] *Dáil Debates*, vol 334 col 1590 (19 May 1982).

[21] *Postal and Telecommunications Services (Amendment) Act 1999*, s 7.

[22] SI 306/2003, s 4(5): "A reference in any enactment to a person licensed under section 111 of [the *Postal and Telecommunications Services Act 1983*] is to be construed as a reference to an undertaking deemed to be authorised under these Regulations."

[23] D Kelleher and M Murray, *IT Law in Ireland* (Dublin: Butterworth, 1997).

Attempts to modify old provisions protecting public utilities appear well-intentioned, but can still cause difficulties. A good example here is section 326(1) of the *Criminal Code* of Canada, where the historical origins are clear.[24]

> *Every one commits theft who fraudulently, maliciously, or without colour of right, (a) abstracts, consumes or uses electricity or gas or causes it to be wasted or diverted; or (b) uses any telecommunication facility or obtains any telecommunication service.*

In this context, one particular case should be considered: inadvertent descrambling of a scrambled TV signal was not covered by this provision; "ensuring adequate scrambling was up to the pay-tv company, as viewers who receive unscrambled signals through no connivance of their own do not offend [this section],"[25] (i.e. by not satisfying the first element (fraud/malice/without right)). Indeed, for those who defend the use of open WAPs, this is in fact quite encouraging as it suggests an approach that would not define such conduct as criminal (at least under this heading).

Finally, in the case of the UK, it must be suggested that Parliament has added additional complexity through enacting section 11 of the *Fraud Act 2006* (dishonestly obtaining services).[26] This general offence (replacing a older offence of obtaining services by deception)[27] is the classic situation whereby a person "orders a meal in a restaurant knowing he has no means to pay,"[28] explained in the explanatory memorandum as including: the use of false payment details or other false personal information to obtain "data or software … made available on the Internet to a certain category of person who has paid for access rights to that service"; decoding television signals "for which [the person] has no intention of paying"; and, curiously, "a situation where a person climbs over a wall and watches a football match without paying the entrance fee – such a person is not deceiving the provider of the service directly, but is obtaining a service which is provided on the basis that people will pay for it."[29] An "act" is required (explained in Parliament as excluding the possibility of guilt based on an omission). This section is potentially capable of capturing unobjectionable Internet use on the same basis as the broad interpretation of section 125. There is also the point that the language of the section, with its reference to "payment having been made" could exclude certain types of fraudulent transaction

---

[24] See generally G Takach, *Computer Law* (Toronto: Irwin, 2003), at 233.

[25] *Ibid,* at 234. The case is *R v Miller and Miller* (1984) 12 CCC (3d) 466 (Alta CA).

[26] On the question of fraud legislation and computers more generally, note that some Commonwealth jurisdictions and Ireland also offer a "dishonest use of a computer" offence as part of fraud legislation: T McIntyre, "Computer Crime in Ireland: A Critical Assessment of the Substantive Law" (2005) 15 *Irish Criminal Law Journal*, 1-10, at 4-5.

[27] *Theft Act 1978*, s 1.

[28] See, e.g. "CPS Legal Guidance: Fraud Act" available at http://www.cps.gov.uk/legal/d_to_g/fraud_act/ (accessed 6 April 2009).

[29] An amendment that would have excluded the viewing of, e.g., a sports match without payment from a suitable vantage point outside of the premises from the section, was not moved at committee stage. The Solicitor General explained that the application of the *Ghosh* test would make this impossible. The scenario used to explain the offence in Archbold 21-404 is that of watching a play in a theatre by gaining access through a fire exit.

where payment is made by an intermediary (e.g. a card issuer).[30] Perhaps this point is also relevant in the case of using paid-for flat-rate Internet access through connection sharing?

3.2 Unauthorised access

The second approach, as suggested above, is to charge the person using an open WAP with an "unauthorised access" offence, of which there is some version in most jurisdictions. It is not yet clear, though, precisely what "access" is being penalised. This brief analysis is thus subject to that essential point being clarified at some future time.

A well-known example of this type of action in the US is the "Peterson incident", where an individual parked outside a cafe using an open WAP apparently without the permission of the WAP admin was convicted of an unauthorised access offence.[31] Although the offences vary from state to state, this particular offence, in Michigan, was in relatively straightforward terms:

> *A person shall not intentionally and without authorization or by exceeding valid authorization . . . access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network.*[32]

Similar provisions are in force in other states and have been used in some cases for relatively minor proceedings.[33] Cannon's analysis of the US position shows that there have been nine prosecutions for access to an open WAP under either state "unauthorised access" provisions or other provisions,[34] pointing out that, while there is some variation between the language, state laws can be classified into two categories: those where the onus is on the individual to establish that access to the open WAP is authorised (29); and those where no such presumption of lack of authorisation operates (11).

Furthermore, the use of "unauthorised access" as the charge is itself controversial in the light of recent developments. Significant attention has been paid to the trial of Lori Drew,[35] who was convicted of misdemeanours (but acquitted of felonies) in

---

[30] D Ormerod, "Response to Letter to the Editor" [2007] *Criminal Law Review*, 662-664.

[31] S Musil, "Michigan Man Dodges Prison in Theft of Wi-Fi" (*CNET News* 22 May 2007) available at http://news.cnet.com/8301-10784_3-9722006-7.html (accessed 6 April 2009).

[32] *Michigan Act 53 of 1979* (as amended), s 752.795.

[33] E.g. E Bangeman, "Illinois WiFi Freeloader Fined US$250" (*Ars Technica* 23 Mar 2006) available at http://arstechnica.com/old/content/2006/03/6447.ars (accessed 6 April 2009).

[34] A more detailed study has been carried out by Cannon and published (as a draft) while this paper was being prepared. I refer the reader to his comprehensive work for further information. Cannon, note 3 above, at 22-23.

[35] Drew was involved in a controversial series of events that included the suicide of a young person (Megan Meier), who had been the subject of bullying though comments sent via MySpace and instant messaging. Drew, along with her daughter and another person, created a profile for a fictitious young person for the purpose of befriending and bullying Meier. See: L Collins, "Friend Game" (*New Yorker*

relation to the Computer Fraud and Abuse Act (CFAA) (unauthorised access offences). As she was said to have violated the MySpace terms of service (by failing to comply with the terms in respect of real identity), authorisation was not "granted" and therefore the use of the service was unauthorised and covered by the Act. This meant that certain of her acts (gathering information on a person) were in violation of the law. For the purposes of the analysis of wifi use, this case is relevant in that it gives a very narrow definition of authorisation and could again expose users of open WAPs to further charges despite thinking that their access is authorised. Of course, US law has also shown itself willing to accept the use of trespass to chattels as an alternative to the CFAA in appropriate cases.[36]

In the UK, the *Computer Misuse Act 1990* creates various offences relating to the use of computers, as its title would indicate. As already noted, it is said that section 1 (as amended by the *Police and Justice Act 2006*) of the Act is engaged by some use of open WAPs:

> *A person is guilty of an offence if (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured; (b) the access he intends to secure, or to enable to be secured, is unauthorised; and (c) he knows at the time when he causes the computer to perform the function that that is the case.*

The Act was the product of quite some discussion with the ability to prosecute "computer crime" – in particular the successful challenge to convictions for what was clearly undesirable conduct not directly covered by existing provisions.[37] There was some disagreement between the Law Commission and Scottish Law Commission on whether there should be a requirement for benefit/loss. The approach of the former (no requirement) prevailed.[38] It is also the case that the original section 1 offence is now triable either way and attracts a penalty of up to two years.

The scope of section 1 is potentially quite broad. In *Ellis v DPP*,[39] for example, the defendant used university computers (which were password-protected but had been left logged on by authorised users). The unfortunate Mr Ellis "drew an analogy between what he did with the computers and picking up someone else's discarded newspaper to read" when interviewed by a police officer.[40] This appears a fair

---

21 January 2008). On the outcome of the case, see "*US v Drew*" available at http://www.citmedialaw.org/threats/united-states-v-drew (accessed 6 April 2009); "Lori Drew Not Guilty of Felonies in Landmark Cyberbullying Trial" available at http://blog.wired.com/27bstroke6/2008/11/lori-drew-pla-5.html (accessed 6 April 2009).

[36] M Wong, "Cyber-Trespass and 'Unauthorized Access' as Legal Mechanisms of Access Control: Lessons from the US Experience" (2007) 15 *International Journal of Law & Information Technology*, 90-128, at 95-105.

[37] The classic example is *R v Gold*, [1988] 1 AC 1063 (HL) (use of a subscription-based database by "hackers" using another person's ID and password).

[38] I Lloyd, *Information Technology Law* (5th ed) (Oxford: OUP, 2008), at 222.

[39] [2001] EWHC Admin 362. See: S Hedley, *The Law of Electronic Commerce in the UK and Ireland* (London: Cavendish, 2007), at 19.

[40] [2001] EWHC Admin 362, at [8].

analogy, but his conviction was affirmed without significant discussion.[41] On a related matter, although the point has not been directly addressed by the courts, it is noted by some scholars that there should be at least a proper notice in place in order for access to be considered unauthorised.[42]

Looking at the approach across the Commonwealth is also helpful. For example, some individuals in Singapore have been charged[43] with an offence under the jurisdiction's *Computer Misuse Act*: "any person who knowingly ... secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service."[44] This offence appears to be based on that of Canada (section 342.1 of the *Criminal Code*, introduced in response to a decision that a "computer" was not a "telecommunications facility" and therefore not covered by existing law),[45] and is similar to offences across the Commonwealth, such as that in New Zealand,[46] though there is still some variation in the level of intent or knowledge required.

In both cases in Singapore, it appeared to be more than mere Internet use at issue (although the networks were in both cases open and unsecured). Garyl Tan Jia Luo was a young person who had been banned from using his parent's Internet connection and was involved in an argument with the owner of the network he was using (a neighbour), while Lin Zhenghuang[47] was said to have posted a bomb hoax for which the WAP admin was initially investigated by the police. Drawing on Cannon's taxonomy discussed above, these offences do appear to have a slightly clearer approach to the question of intention (although there are potentially significant differences between them).[48]

---

[41] In this unusual case there was also the suggestion from the defence that "browsing" alone would not constitute "use" for the purposes of the *Computer Misuse Act*. The matter turned on whether the defendant launched an application or merely used an application already open. Whether this is a proper reflection of the reality of computer use is questionable. Any conclusions that could be drawn are, however, very much hindered by the fact that Ellis was not represented at the scheduled hearing. At a further hearing ([2002] EWHC 135 (Admin)) he was, though the extent to which these arguments were pursued is unclear.

[42] Lloyd, note 38 above, at 225; C Gringas and E Todd, *Gringras on the Laws of the Internet* (3rd ed) (Haywards Heath: Tottel, 2008), at 297.

[43] G Kennedy and S Doyle, "A Snapshot of Legal Developments and Industry Issues Relevant to Information Technology, Media and Telecommunications Law in Key Jurisdictions Across the Asia Pacific – Co-ordinated by Lovells and Contributed to by other Leading Law Firms in the Region" (2007) 23:3 *Computer Law & Security Report*, 238-247, at 245.

[44] Section 6(1).

[45] *R v McLaughlin*, [1980] 2 SCR 331.

[46] "[W]ho intentionally accesses, directly or indirectly, any computer system without authorization, knowing that he or she is not authorized to access that computer system, or being reckless as to whether or not he or she is authorized to access that system": *Crimes Amendment Act 2003*, s 252.

[47] See also D Ho "Singapore Man Jailed For Tapping Network" (*Washington Post* 7 February 2007) available at http://www.washingtonpost.com/wp-dyn/content/article/2007/02/07/AR2007020701338.html (accessed 6 April 2009).

[48] For example, it has been argued that the Singapore offence is more difficult to prove, as it appears to suggest that knowledge is required in respect of the act of computer use as well as the purpose of securing obtaining access: Wong, note 36 above, at 118.

It does seem inappropriate, though, to charge the "misusers" by using an offence that is, by its terms, not limited to inappropriate use or situations of dispute between the user and the owner of the router. What this approach does is classify a wide range of people as engaged in criminal conduct (to which there may be no obvious defence) with a seeming reassurance that the offence is only prosecuted where other factors are present. Indeed, given that new devices such as the iPhone are set up not just to connect to available open networks but to swap with ease between mobile and wifi networks – a developing trend across a range of devices – and efforts have been made to collect all sightings of open WAPs[49] – there is no excuse for ignoring the fact that countless users will be using open networks on a regular basis. As with the discussion of the network use offences above, the purpose of the statute deserves consideration. The *Computer Misuse Act* is about the "protection of the integrity and security of computer systems."[50] Is this the most appropriate way to regulate wifi sharing?

4. The position of the WAP admin

Even if all issues relating to the use of the open WAP by the passing stranger were resolved, there would still be questions to consider regarding the WAP admin. This means that it remains difficult to advise the ISP's customer on what course of action is advisable. One particular question that faces the person who owns the router and pays for the Internet connection – aside from any issues associated with the use of the connection by others – is that of liability. In debates over the introduction of new measures to restrict the downloading of material in violation of copyright law, the question of what sort of responsibility the customer of the ISP has for the actions of others using an open WAP has arisen. Unfortunately, it does seem that the "solution" to the question – from the point of view of those who would support the "graduated response" of cutting off the Internet access of alleged infringers – is to instruct or require the customer to secure their WAP in order to avoid incurring liability or disconnection.

Limited consideration was given to a slightly different question in the US – the unsuccessful raising of the possibility of third-party use by a WAP admin charged with child pornography offences (in the context of a challenge to a warrant which, it was argued, was incorrectly issued). This does point to potential division. The US finding could be seen in a different light, though, in that the possibility of third-party use was not enough to displace the lower requirement (probable cause, which is some distance from "beyond a reasonable doubt") for the issue of a warrant. The conviction itself in this case was supported by significant evidence and other factors.[51] A similar argument was alluded to, but not accepted, in the English case of *Ashton v Rusal*.[52] In this case, an action including a claim based on breach of confidence was commenced.

---

[49] W Gardner, "Worldwide Wi-Fi Social Network Takes Off" (*Information Week* 25 November 2008) available at http://www.informationweek.com/news/mobility/wifiwimax/showArticle.jhtml?articleID=212200470 (accessed 6 April 2009).

[50] N MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" [2008] *Criminal Law Review*, 955-967, at 957.

[51] *US v Perez*, 484 F.3d 735 [13-14] (5th Cir 2007).

[52] [2006] EWHC 2545 (Comm), at [39]-[42], [51].

One argument advanced (at an early stage, in this reported decision dealing primarily with jurisdiction) by the defendants was that they could not be responsible for the alleged breach (access to the applicant's computers by the defendant) as the defendant's network (in Russia) included a WAP near to a university. The defendant's case was not assisted by the fact that the network was partially secured (MAC authentication) and thus the scenario would involve not just MAC address spoofing but also that it happened in (apparently clearly proven) access to the applicant's computers (in the UK), with the parties being in the progress of long, bitter litigation on various matters. Hirst QC (sitting as deputy judge) agreed that the applicants had shown that there was a serious issue to be tried. The case, then, is of some interest. Nevertheless, it is unlikely to be a controlling precedent in more ambiguous cases – an encouraging point in light of the criticism of the section 125 and *Computer Misuse Act* cases discussed above.

Aside from questions of legal liability, there have been a number of influential statements (particularly from the computer security industry) that encourage WAP admins to secure their networks. This is generally on the grounds that failing to do so compromises the security of data on the WAP admins' computers and can also allow malicious users to "eavesdrop on communications."[53] This was achieved by force of law in India earlier this year, where it was reported that police made use of a general provision on crime prevention ("Every police officer may interpose for the purpose of preventing, and shall, to the best of his ability, prevent, the commission of any cognizable offence"): "If a particular place's Wi-Fi is not password protected or secured then the policemen at the spot has the authority to issue notice to the owner of the Wi-Fi connection directing him to secure the connection."[54] Again, if it is necessary for the actions of the WAP admin to be restricted, this should not be by fiat any more than it should be by contract. Finally, some research indicates that WAPs are a point of vulnerability in a coordinated attack – with some modelling of data in New York suggesting that modification of firmware on a large scale would be rapid and not particularly difficult.[55] However, even in the light of widespread concern about reliability and emergency management, it should be remembered that there are many "vulnerable" systems (demonstrated in a number of the prominent attacks on or using transport in New York, Madrid and London) and a response should thus be considered in the light of the rapid change in the working methods of those who would engage in criminal conduct, balanced with the social harm caused by restrictive measures. Turning off and smashing up all the routers would, of course, guarantee no hacking.

The "open" approach still prevails in the cases of some prominent bloggers and activists, who declare that they have made a conscious choice to provide an open network through their router.[56] Indeed, while large-scale and credible research is

---

[53] Sophos, note 7 above.

[54] "Mumbai Police to look out for Unsecured Wi-Fi Connections" (*Times of India* 9 January 2009) available at http://timesofindia.indiatimes.com/Cities/Mumbai_cops_probing_Wi-Fi_security/articleshow/3956633.cms (accessed 6 April 2009).

[55] H Hu et al, "WiFi networks and malware epidemiology" (2009) 106:5 *Proceedings of the National Academy of Sciences*, 1318-1323.

[56] B Schneier, "Security Matters" (January 2008) available at http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0110 (accessed 6 April 2009).

required, even the anecdotal work carried out to date indicates that a significant proportion of WAP admins do not secure their network (whether by deliberate choice or non-action – i.e. accepting the default settings).[57] A middle path is suggested by the requirement in California that relevant equipment (WAPs, essentially) be labelled with information on how to secure (close) the network.[58] However, some ISPs are still quite adamant on the matter. Although practice has varied over time,[59] some still restrict through terms of service.[60] It is fair to wonder whether these terms are notified to users in an appropriate fashion for the purposes of the law on consumer contracts as they may indeed be quite restrictive and onerous. Take, for example, the UK ISP Karoo, which currently requires its customers to agree that: [61]

> *[Karoo] shall be entitled to terminate the Service immediately if We discover that . . . you have permitted (whether knowingly or not) a third party (or third parties) to access the Service using a wireless connection over Your Communications Line.*[62]

Along with a possible "requirement to close," though, there is the further question of the status of the WAP admin. On a number of occasions, it has been suggested by commentators that WAP admins providing open networks would be engaged in the providing of a service for the purposes of (US) federal law and thus would be subject to a financial penalty for failure to comply with monitoring obligations. This is confused by the fact that the provisions supposedly creating obligations for the subscriber were already in force and the Act was extending the obligations and penalties without a change to the underlying definitions.[63] In the context of the introduction of "data retention" legislation, this is a question of some concern: is the café owner, or indeed the private householder, to be subject to the same obligations as the market-leading ISP?[64]

---

[57] Sophos, note 7 above; H Sathu, "WarDriving: Technical and Legal Context" (2006) *Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics*, 162-167.

[58] *Business and Professions Code*, s 22948.5.

[59] Compare, e.g. "Wi-Fi Friendly ISPs" (2002) available at http://www.dslreports.com/shownews/23656 (accessed 6 April 2009); "Which ISPs Allow Sharing?" (2004) available at http://wifinetnews.com/archives/2004/05/which_isps_allow_sharing.html (accessed 6 April 2009); "Wi-Fi service breaches ISP conditions" (*OutLaw*, 2007) available at http://www.out-law.com/page-7335 (accessed 6 April 2009).

[60] On terms of service generally, see: S Braman, "Advantage ISP: Terms of Service as Media Law" (2003) 5:3 *New Media & Society*, 422-448.

[61] It is alleged that the impetus for this new restriction is the concern expressed by legal representatives of copyright holders (i.e. music & entertainment industries) that open WAPs hamper legal actions (as discussed earlier in this paper). See: "ISP Disconnects Customers with Open WiFi" (November 2008) available at http://torrentfreak.com/isp-disconnects-customers-with-open-wifi-081102/ (accessed 6 April 2009).

[62] http://www.karoo.co.uk/pdf/karoo-broadband-standard-terms-november-2008.pdf (accessed 6 April 2009), at 9.6.4(iii).

[63] D McCullagh, "House Vote on Illegal Images Sweeps in Wi-Fi, Web Sites" (*CNET* 5 Decembers 2007) available at http://news.cnet.com/8301-13578_3-9829759-38.html (accessed 6 April 2009).

[64] D McCullagh, "Bill Proposes ISPs, Wi-Fi Keep Logs for Police" (*CNET* 19 February 2009) available at http://news.cnet.com/8301-13578_3-10168114-38.html (accessed 6 April 2009). On the approach taken by law enforcement to the definition of an electronic communications service under US law, see:

On the other hand, should the open network be an electronic communications service, then it may be protected by provisions such as Article 12 of the E-Commerce Directive[65] as a mere conduit. One factor of possible note from an EU point of view is whether the service is provided "for remuneration" (an essential component of EU law due to the requirement for a Treaty basis – i.e. the provision of Treaty services). It has been suggested that where there is an "exchange relationship" (where mutual access is granted within an organisation or pursuant to an agreement), this element is satisfied.[66] It is submitted that, if this is the case, organisations involved in such activities must give detailed consideration to the rights and obligations of EU law that would be triggered by a decision to participate.

5. Municipal and Community Wifi

5.1 Introduction

Wireless access is not just about domestic WAPs, though. Over the past few years, there has been a great deal of excitement – and scepticism – over the possibility of wireless Internet access being provided across a wide area (in particular where the provider is a local governmental authority). Referred to as "municipal wifi," the idea is attractive in that it brings together concepts of new technology, localism and a right of access. However, it is also a significant threat to the established players in the Internet access market, who are naturally suspicious of anything that looks like State intervention or subsidy. Indeed, the concerns raised relating to competition law have been a major – and, it is argued, disproportionate – factor in the development of municipal wifi proposals.

It is not intended to argue that competition law has no role to play, but instead that other rationales for the various projects, particularly those in relation to access to information and cultural participation, have been played down and disregarded. This makes it seem to the casual observer that the purpose of the legal interventions into municipal wifi is the protection of incumbent ISPs. One example of a broader social purpose to wide availability of Internet access through wifi is the role it plays in the construction of public space. Two competing possibilities on what this means are suggested by Hampton and Gupta in an ethnographic study of the use of wifi in public and semi-public spaces: that the wide availability of wifi will encourage greater participation in public spaces; and that said use will further the trend towards private interaction (distracting the user from interacting with co-present others).[67] The research that they carried out indicated that there was a distinction between two

---

"Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (Computer Crime & IP Section, Dept of Justice, 2002) available at http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm (accessed 6 April 2009), at III-B.

[65] *Directive 2000/31/EC of the European Parliament and Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML.

[66] R Robert et al, "Wifi Roaming: Legal Implications and Security Constraints" (2008) 16:3 *International Journal of Law & Information Technology*, 205-241, at 221.

[67] K Hampton and N Gupta, "Community and Social Interaction in the Wireless City: Wi-Fi Use in Public and Semi-Public Spaces" (2008) 10:6 *New Media & Society*, 831-850, at 836.

classes of users – true mobiles and placemakers – who were both present in the same space as observed. Powell has recently made the case that the better model is that of community wifi as more akin to a public park, providing a space for creativity.[68] There are also different approaches taken as to the use of open networks provided by locations such as coffee shops: some take no action; others use it creatively as a way of advertising their core products (such as naming the WAP with an advertising slogan like HaveYouTriedTheCarrotCake);[69] while others again take steps to discourage ongoing use, such as the removal of power outlets, communicated rules, limiting use during peak hours, and informal staff actions ("can I get you anything else") designed to dissuade non-purchasing occupants from continuing their use and taking up a space that could be used by a paying customer.[70]

5.2 Competition law in Europe

The European Commission has had cause to address this issue through the application of its competition law powers. One particular project, in Prague,[71] was given a "conditional approval"[72] but, in practice, this was a fundamental change in the municipal wifi model. The conditions were so onerous as to move the project from "Internet access" to a very limited, content-specific service – the difference, perhaps, between a local authority opening a library primarily supplying the books of others and putting up a simple billboard with information leaflets. While it is understandable how advocates of the proposals would like to see the positive aspects of the Commission's decision (and the Commission itself was at pains to point out that it was not rejecting the scheme), this is in reality a defeat for the philosophy that Internet access itself is a tool for empowerment and a proper concern of progressive local authorities.

The Commission found that the Prague proposal, intended to provide for Internet access in general, could only go ahead if it was limited to use by public servants in the performance of their duties (a contemporaneous proposal from the Welsh Assembly for a similar purpose was also approved by the Commission), or use by the general public but limited to accessing Government websites. It is the latter aspect that is deserving of particular attention. The idea that the Internet can be so neatly subdivided – Government websites and other websites – flies in the face of any reasonable person's observation of Internet use. Of course, Government websites are

---

[68] Powell, note 3 above. On this argument, see also A Sanusi and L Palen, "Of Coffee Shops and Parking Lots: Considering Matters of *Space* and *Place* in the Use of Public Wi-Fi" (2008) 17 *Computer Supported Cooperative Work*, 257-273 (exploring legitimacy and hospitality and the development of social habits and practices in commercially-mediated "free" wifi spaces).

[69] "This is what I call inventive…" (*Swissmiss* 2008) available at http://www.swiss-miss.com/2008/12/this-is-what-i.html (accessed 6 April 2009).

[70] Hampton & Gupta, note 67 above, at 846.

[71] Wireless Prague, "Municipal Wireless Broadband Internet Project for Citizens, Tourists and Local Government" available at http://wifi.praha-mesto.cz/default.aspx?ido=70&sh=220781691 (accessed 6 April 2009).

[72] European Commission, Decision by DG Competition, "State Aid NN 24/07- Czech Republic Prague Municipal Wireless Network" (30 May 2007), NN 24/07: OJ C 141/1, available at http://ec.europa.eu/competition/state_aid/register/ii/by_case_nr_nn2007_0000.html#24 (accessed 8 July 09).

of particular importance in terms of the citizen's relationship with the State and restriction of access to them is, prima facie, troubling. There is, however, no "Government Internet" from the point of view of the user (indeed, public sector websites could only be defined by way of a compiled list in many jurisdictions, given the diversity of domain names now in use) and the rationale for supporting access to the Internet does not break into the easy categories that the Commission would believe. Indeed, in the context of the history of freedom of expression, creating a separate category for one-way Government expression is itself quite dangerous, in that it encourages the creation of a specific path for the State expressing itself to citizens, but little ability for the citizen to criticise or respond. The user of municipal wifi under the Prague compromise is thus free to read the press release of a Minister, but not to write a blog entry criticising it or watch a video clip posted by an opposition party. This would be disturbing as applied to conventional forms of media, but in the case of the Internet is beyond baffling. The Commission's arguments are necessarily surreal, arguing that the project is acceptable because there will be no advantages to the providers of public sector websites or to website users of allowing access![73]

On the other hand, supporters of the Prague decision can easily point to the development of modern telecommunications networks across Europe as a result of the progressive liberalisation of the various national markets and the restrictions on the incumbent (and often State-owned or formerly State-owned) enterprises. The present situation in many member states is characterised by a diversity of providers and an apparent incentive for investment and technological development, although this has been questioned by some. Certainly, care should be taken not to disturb this although, as the power of the incumbents diminishes, concerns must also be raised that a system based on a number of private providers and little public involvement substitutes a dominant ideology (the free market of retail ISPs) for a dominant player (the incumbent telecommunications operator). A compromise (perhaps based on careful use of tendering) may yet be possible. This does require some speedy action; the Prague decision has also had an impact on other proposals, without requiring formal intervention by the Commission. For example, a planned network in Dublin was abandoned at a relatively early stage[74] as it was clear to those concerned that the project was too similar to that originally proposed by Prague. The local authority decided instead to explore other options such as free Internet access in libraries – which itself is interesting, as libraries themselves do appear to be inconsistent with the strict application of competition principles. Furthermore, the idea of walk-in Internet access (even for fixed, desktop machines) is the business model of the cybercafé as well as the familiar feature of the modern library. It is unfortunate that there has not been a clear ruling on this point. Indeed, the Dublin decision not to proceed was the subject of criticism from unlikely sources, such as the local Chamber of Commerce.[75] Meanwhile, in the US, a number of states have intervened to prohibit municipalities

---

[73] *Ibid*, at 8.

[74] "No Free Wi-Fi for Dublin" (*RTE News* 9 January 2008) available at http://www.rte.ie/news/2008/0109/wifi.html (accessed 6 April 2009).

[75] "Nine questions for... Gina Quin" (*RTE News* 21 January 2008) available at http://www.rte.ie/news/2008/0121/quing.html (accessed 6 April 2009).

from developing networks.[76] Interestingly, the economic basis for restricting State investment is being challenged[77] and there is also some diversity in the models adopted by cities,[78] indicating that there may indeed be no single reason that public authorities should not have an interest in the area.

It can be said that the strict application of competition law principles (or specific statutory restrictions on investment) play a similar role to the overextension of criminal offences regarding use of communications services and unauthorised access, in that the legal moderation of end-user behaviour is designed to protect "the network" (or, in reality, the network provider – the ISP) without regard to how this affects the ability of the end-user to use the Internet. If this position was ever defensible, it is questionable whether it is of any value today. Even accepting the success of liberalisation in the European Union (which, of course, is not replicated in other jurisdictions such as the US, where choice is still limited in many areas), it may be necessary to reformulate the issue as one of mixed telecommunications and media/information elements, recognising that competition law in the case of 'pure' media has long attracted special provisions with regard to the cultural and social importance of media pluralism. If Internet access is only seen by the law as a by-product of the more important policy object of network protection, this will not be possible.

5.3 Other issues

Projects in the US have also failed to develop as expected in many cases, with the plans being described in the New York Times as "tripped up by unrealistic ambitions and technological glitches."[79] The key weakness in many US proposals appears to have been the agreements with private sector providers. These became the subject of disputes with the commissioning authorities – particularly in relation to cost and profitability. It is also the case that the reported reduced cost to the consumer of Internet access per se and also wireless connectivity in particular has had an impact on the demand (and thus the incentive for public-private partnerships) for municipal services, which could mean that one of the reasons for State intervention in the US (the high cost of Internet access) is being addressed through other means (i.e. increased competition between Internet service providers). That said, there are ongoing concerns regarding the cable/digital subscriber line (DSL) duopoly in the US, and the prospect of addressing this through municipal wifi appears to no longer be a realistic one.

---

[76] A Tapia and J Ortiz, "Municipal Responses to State-Level Broadband Internet Policy," *Proceedings of the 34th Telecommunication Policy Research Conference* (Sept-Oct 2006) available at http://web.si.umich.edu/tprc/papers/2006/554/TPRCfinal_pdf.pdf (accessed 6 April 2009).

[77] See: G Ford, "Does Municipal Supply of Communications Crowd-Out Private Communications Investment? An Empirical Study" (2006) available at http://ssrn.com/925970 (accessed 6 April 2009).

[78] F Bar and N Park, "Municipal Wi-Fi Networks: The Goals, Practices, and Policy Implications of the U.S. Case" (2006) 61 *Communications & Strategies*, 107-125.

[79] I Urbina, "Hopes for Wireless Cities Fade as Internet Providers Pull Out" (*New York Times* 22 March 2008) available at http://www.nytimes.com/2008/03/22/us/22wireless.html (accessed 6 April 2009); for a more optimistic take on the same facts, see C Aaron, "The Promise of Municipal Broadband" (*The Progressive* August 2008) available at http://www.progressive.org/mag/aaron0808.html (accessed 6 April 2009).

There is also the important question of what level of filtering, if any, is permissible. Given that municipal wifi and other collectively managed wireless internet services involve some measure of administrative oversight, the temptation to restrict use is clearly significant. In Powell's study of municipal wifi projects in two Canadian cities, she finds that users on the network characterised by a greater degree of freedom were three times more likely to create and distribute original (user-generated) content.[80] On the other hand, the impact of the launch of "in-flight" wireless Internet access was diminished by the acknowledgement that such access would be filtered (for decency as well as commercial purposes, i.e. pornography and Voice over Internet Protocol (VOIP))[81] above and beyond the normal practices of "wired" ISPs on the ground, despite no legal requirement for such. Restrictions on peer-to-peer use (whether legal or otherwise) are unfortunately common, as is increasingly the case for established (DSL/cable) broadband ISPs too.[82]

5.4 Sharing – the key to municipal wifi?

Furthermore, it is contended that there is the possibility for useful interaction between the "wifi sharing" and "municipal wifi" debates. The first wave of development is that related to communities like FON,[83] where WAP admins agree to establish a FON-enabled WAP (though only open to other FON members, and protected by various security devices). In return, the member is assured that they can make use of the WAPs of other FON members around the world. It is also possible for WAP admins to earn money through the system by allowing users ("Aliens") who have purchased a "FON pass" (i.e. a user who is not sharing through their own WAP but wishes to use the admin's WAP). Of course, the contractual restrictions of the ISP are relevant: FON requires participating WAP admins to "check if you are permitted to share bandwidth in accordance with your ISP user agreement as you are solely responsible for compliance with the ISP´s contractual obligations." FON is a serious player backed by familiar names such as Google and Skype and participating in joint agreements with the likes of ISP BT. The BT agreement is particularly interesting, with users being able to opt in (or from March 2009, be automatically opted-in!)[84] to the "BT FON community," where they will provide access to the Internet through their BT-supplied Internet connection through a FON-enabled WAP and be able to

---

[80] Powell, note 3 above. For another perspective on these networks, see: C Middleton and B Crow, "Building Wi-Fi Networks for Communities: Three Canadian Cases" (2008) 33:3 *Canadian Journal of Communication*, 419-441.

[81] M Maynard, "Not Everyone Is Cheering as Wi-Fi Takes to the Air" (*New York Times* 6 February 2009) available at http://www.nytimes.com/2009/02/07/business/07plane.html (accessed 6 April 2009).

[82] T Wu, "Network Neutrality, Broadband Discrimination" (2003) 2 *Journal of Telecommunications & High Technology Law*, 141-179; C Marsden, "Net Neutrality and Consumer Access to Content" (2007) 4:4 *SCRIPTed*, 407-435.

[83] http://www.fon.com (accessed 6 April 2009). See, generally: J Markoff, "Global Dreams for a Wireless Web" (*New York Times* 25 May 2008) available at http://www.nytimes.com/2008/05/25/technology/25web.html (accessed 6 April 2009).

[84] Note also that BT is implementing a non-FON system whereby business users of its DSL service will see their existing WAPs used as BT Openzone (commercial wifi) access points. B Ray, "BT Reprograms Biz Customers at Hotspots" (*The Register* 27 February 2009) available at http://www.theregister.co.uk/2009/02/27/bt_business_fon/ (accessed 6 April 2009).

use FON WAPs around the world. This tolerated sharing, in the context of the application of section 125 of the *Communications Act*, adds further confusion.

However, in general it can be said that FON's business model is still under debate,[85] and it is more properly described as a semi-open system, in that the WAP is typically "closed" but can be used through authentication. Additionally, a second wave is now with us. Useful work has been carried out to build a technical and policy template for "tunnelling" – a system whereby the user connects to an open WAP and onwards through a secure connection to an existing access point of their own (e.g. their home ISP). This approach protects both the WAP admin and the user against certain legal and security risks.[86] This is argued to be of particular relevance within a community of interest where mutually convenient access is granted to members, with the membership being voluntary but based on a general organisation (or even a specific geographic region such as a municipality). In the context of difficulties experienced by municipal wifi project and the increasing availability of domestic WAPs, this approach – and that of FON and its alternatives – may become more significant. It is suggested that further clarification on the outstanding legal aspects (such as the power of the municipal authority to establish such a scheme, or indeed the inconsistent application of access and network provisions of criminal law) would be significantly beneficial to proponents of both FON-like systems and also the tunnel-based solutions.

5.5 White spaces?

It is obvious that the very idea of wide-area wireless Internet access remains a compelling one. Various attempts have been made to make this a reality, such as WiMax and other projects, and increasingly the use of 3g services supplied by mobile phone operators (to "ordinary" consumers as well as users of smartphones, etc). The project that has been the subject of much attention over the past year, though, is the use of part of the soon-to-be-vacated spectrum presently allocated for traditional over-the-air analogue ultra high frequency (UHF) television (TV) broadcasting.[87] Part of this spectrum, referred to as 700MHz or "white spaces" could be used for "unregulated" broadband access (i.e. permitted unlicensed use along similar lines to wifi at 2.4GHz but with the potential for high quality and good distance). It is the subject of policy processes in various jurisdictions, most notably in the US.[88] This has highlighted the difficult challenge for regulators in controlling competing claims for access to spectrum while also playing a part in a more general debate about Internet access and broadband competition. The pace of development here has been rapid,

---

[85] Markoff, note 83 above.

[86] N Sastry, J Crowcroft and K Sollins, "Architecting Citywide Ubiquitous Wi-Fi Access" (2007) *Proceedings of the 6th ACM Workshop on Hot Topics in Networks (Hotnets-VI)* available at http://conferences.sigcomm.org/hotnets/2007/papers/hotnets6-final88.pdf (accessed 6 April 2009). See also: Robert, note 66 above.

[87] See, e.g. "Google Plan Would Open TV Band for Wireless Use" (*New York Times* 25 March 2008) available at http://www.nytimes.com/2008/03/25/business/media/25google.html (accessed 6 April 2009); "Wireless at Warp Speed" (*The Economist* 7 November 2008) available at http://www.economist.com/displayStory.cfm?story_id=12581204 (accessed 9 July 2009).

[88] Approved by the FCC in November 2008 (FCC 08-260); various applications to challenge the decision are pending in US federal courts at the time of writing.

with devices tested in late 2008 appearing to address most of the complaints made by incumbent users of the spectrum at issue.[89]

Indeed, some players such as Google (consistent supporters of alternative forms of Internet access for various reasons) suggest that there is a link between the goals of municipal broadband and the parallel debate on the use of the white spaces[90] and its founder lauds the decision to open up this spectrum as a victory for "science over politics."[91] However, aside from Google's (understandable) economic self-interest in high-speed Internet access being available to users, it is obvious that there is a strong political dimension to the "white spaces" proceedings as part of the broader consideration of the role of Internet access. Choosing neither to allocate nor to auction but, instead, to designate for use by (partially regulated) devices requires concerted political effort and an understanding of communications policy. It is, by Federal Communications Commission (FCC) standards, a relatively risky approach. Separately, it has been criticised by some parties (broadcasters, as well as current users of spectrum for short-range devices such as wireless microphones).

6. Conclusion

It is suggested that the thread (or cloud?) connecting domestic WAPs, municipal wifi and spectrum reform is a desire to enable the use of the Internet by individuals, rather than the management of a network in the interests of service providers. Some of the legal provisions criticised in sections 3 and 4 are more appropriate to large, discrete networks rather than the flexible, atomised wireless commons. Consider instead, however, a situation where the law protected the ability of the WAP admin to share and the external user to connect, and where analyses of spectrum allocation and competition law could be informed by a declaration (whether administrative statutory, constitutional or mere policy) that providing access to the Internet with the maximum possible freedom of action and of use reserved to the user was itself important. In the context of rules on state aid which might hamper municipal wifi, this is clearly important. In addition, below the surface of the white spaces debate was the idea that those opposed to current ISP policies could built a "freer" network at 700MHz. This, though, is by no means a foregone conclusion.

The advantages of a coherent approach either driven by community organisation or democratically accountable local governmental authorities is apparent – nothing should stop the café owner from choosing one model or the other. If, however, the social goals of increased Internet access are to be met, it cannot be left to the mercy of the ups and downs of the caffeinated beverages industry. White spaces Internet access may be better, though – despite the premature declaration of victory of November 2008 – there are important decisions to be made in that regard too. The potential for

---

[89] K Greene, "The Coming Wireless Revolution" (*Technology Review* November 2008) available at http://www.technologyreview.com/communications/21671/ (accessed 6 April 2009).

[90] D Slater, "'The Promise of Municipal Broadband' & white spaces" available at http://googlepublicpolicy.blogspot.com/2008/08/promise-of-municipal-broadband-white.html (accessed 6 April 2009).

[91] L Page, "A Vote for Broadband in the 'White Spaces'" available at http://googleblog.blogspot.com/2008/11/vote-for-broadband-in-white-spaces.html (accessed 6 April 2009). Page is a co-founder of Google.

the social benefits of increased and encouraged "calculated co-presence"[92] (where individuals share physical and social spaces but are able to pursue a range of goals including in conjunction with others in a different space) must be an ever present reminder of what we are seeking. Inappropriate legal constraints on or actions against WAP admins, wifi users or public authorities acting in the best traditions of the local library or park (if one may be permitted to use a metaphor!) are a clear and present threat to this model. An evolving regulatory understanding of the purpose of Internet access, suggested in the white spaces decision, hints at a possible way forward.

[92] *Networked Publics*, note 8 above, at 16-17.